Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/679,333	10/04/2000	Stefan Hepper	DE919990073US1	6558

46369	7590	07/27/2005

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/679,333	HEPPER ET AL.
	Examiner	**Art Unit**	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   Applicant's amendment filed 26 April 2005 amends claims 1-3, 6-8, 10, 14, 17-20.
filed ꬳꬳꬳ as per RCE of 6/20/2005
Applicant's amendment has been fully considered and is entered.

Response to Arguments

2.   Applicant's arguments filed 26 April 2005 have been fully considered but they are not

persuasive.

3.   In response to applicant's argument that the references fail to show certain features of

applicant's invention, it is noted that the features upon which applicant relies (i.e., processing

protocol between the server and terminal which would minimize data transfers between the

server and the client, the terminal being able to read the content of the messages from the server)

are not recited in the rejected claim(s). Although the claims are interpreted in light of the

specification, limitations from the specification are not read into the claims. See *In re Van*

Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4.   Applicant's argument that Chen discloses a memory chip card instead of a smart card is

insignificant because one cannot show nonobviousness by attacking references individually

where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413,

208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). Peyret discloses a method for loading applications onto a smart card wherein the system

includes a smart card, terminal (client), and a server (Fig. 4). Peyret does not disclose that the

application is unpacked at the user terminal before being installed on the smart card. Chen

discloses a method for installing an application wherein a desktop manager on the user terminal

unpacks the application program before installing the program on the memory card (Col. 8, line

66 – Col. 9, line 22). It would have been obvious to one of ordinary skill in the art at the time the

invention was made to unpack the application program of Peyret on the user terminal before

transferring the application to the smart card in order to minimize the decisions required of a user

when installing an application as taught in Chen (Col. 9, lines 24-26).

5.   Applicant's argument that the motivation to combine the Peyret and Chen references is

deficient because minimizing decisions required of a user is not relevant to the claimed

functionality of Applicant's process is not persuasive because the question of motivation is not

whether it is relevant to the claimed invention, but whether one of ordinary skill in the art would

have been motivated to combine the teachings of the references. Minimizing decisions required

by computer users has been at the focal point of computer innovation since the dawn of the

personal computer.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

7.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.

       4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

8.   Claims 1, 4, 6, 8, 12-15, 17, 18, 20 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No.

6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529. Referring to claims 1, 4,

6, 12-15, 17, Peyret discloses a method for loading applications onto a smart card wherein the

system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first

interface system that may connect the smart card to the terminal and second interface to connect

the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the

terminal, the processor of the smart card, verifies the authenticity of the terminal and of the

server and visa versa. If the server and the smart card authenticate each other, then the loader

within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is

selected, which meets the limitation of loading a sequence of commands to download the

application component to the chipcard, to be loaded the smart card authenticates the application

code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private

or secret keys, which meet the limitation of delivery of a secret key or session key by the server,

generation of a digital signature with the secret key or session key by way of each command

within the command sequence, transmission of the signed command sequence as a data packet to

the client. If the digital signature is valid then the application is loaded onto the smart card (Col.

9, lines 54-57), which meets the limitation of checking of the digital signature and execution of

the commands if the digital signature is correct. Peyret does not disclose that the application is

unpacked at the user terminal before being installed on the smart card. Chen discloses a method

for installing an application wherein a desktop manager on the user terminal unpacks the

application program before installing the program on the memory card (Col. 8, line 66 – Col. 9,

line 22), which meets the limitation of unpacking of the data packet by the client and

transmission of the individual commands in sequence to the smart card. It would have been

obvious to one of ordinary skill in the art at the time the invention was made to unpack the

application program of Peyret on the user terminal before transferring the application to the

smart card in order to minimize the decisions required of a user when installing an application as

taught in Chen (Col. 9, lines 24-26). Peyret does not disclose that each individual instruction of

the application is digital signed. Zumkehr discloses a system for error detection wherein

individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47).

It would have been obvious to one of ordinary skill in the art at the time the invention was made

for the application instructions of Peyret to be digitally signed in order to provide low detection

latency as taught in Zumkehr (Col. 2, lines 47-50).

Referring to claim 8, Peyret discloses that the cryptosystem used can be a public key

cryptosystem (asymmetrical) (Col. 5, lines 31-33).

9.   Claims 2, 7, 10, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in

view of Zumkehr, U.S. Patent No. 5,974,529 as applied to claims 1-3, 17 above, and further in

view of Everett, U.S. Patent No. 6,575,372. Referring to claims 2, 7, 10, 19, Peyret discloses a

method for loading applications onto a smart card wherein the system includes a smart card,

terminal (client), and a server (Fig. 4). The smart card has a first interface system that may

connect the smart card to the terminal and second interface to connect the terminal to the server

(Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of

the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the

server and the smart card authenticate each other, then the loader within the smart card begins

the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the

limitation of loading a sequence of commands to download the application component to the

chipcard, to be loaded the smart card authenticates the application code through the use of digital

signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the

limitation of delivery of a secret key or session key by the server, generation of a digital

signature with the secret key or session key by way of each command within the command

sequence, transmission of the signed command sequence as a data packet to the client. If the

digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57),

which meets the limitation of checking of the digital signature and execution of the commands if

the digital signature is correct. Chen discloses a method for installing an application wherein a

desktop manager on the user terminal unpacks the application program before installing the

program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of

unpacking of the data packet by the client and transmission of the individual commands in

sequence to the smart card. Zumkehr discloses a system for error detection wherein individual

program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). Peyret does

not disclose that the keys are generated based on card identification data. Everett discloses an IC

card loading system wherein to generate cryptographic keys for each individual IC card, a

certificate authority uses card identification information transmitted from the terminal in order to

generate individual key sets for the IC cards (Col. 5, lines 42-67). It would have been obvious to

one of ordinary skill in the art at the time the invention was made for the cryptographic keys of

Peyret to be generated based on the IC card identification data in order to easily identify and

authenticate the cards at a later point in time as taught in Everett (Col. 8, lines 25-34).

10.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S.

Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of

Zumkehr, U.S. Patent No. 5,974,529 as applied to claims 1, 13 above, and further in view of

Hanel, GB 2,314,948. Referring to claim 16, Peyret discloses a method for loading applications

onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig.

4). The smart card has a first interface system that may connect the smart card to the terminal

and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When

the smart card is connected to the terminal, the processor of the smart card, verifies the

authenticity of the terminal and of the server and visa versa. If the server and the smart card

authenticate each other, then the loader within the smart card begins the loading process (Col. 7,

lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of

commands to download the application component to the chipcard, to be loaded the smart card

authenticates the application code through the use of digital signatures (Col. 9, lines 50-53).

Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret

key or session key by the server, generation of a digital signature with the secret key or session

key by way of each command within the command sequence, transmission of the signed

command sequence as a data packet to the client. If the digital signature is valid then the

application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of

checking of the digital signature and execution of the commands if the digital signature is

correct. Chen discloses a method for installing an application wherein a desktop manager on the

user terminal unpacks the application program before installing the program on the memory card

(Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by

the client and transmission of the individual commands in sequence to the smart card. Zumkehr

discloses a system for error detection wherein individual program instructions are digitally

signed and later authenticated (Col. 2, lines 29-47). Peyret does not disclose using message

authentication codes in the command codes. Hanel discloses a chipcard data transfer method

wherein message authentication codes are appended to commands (Page 1). It would have been

obvious to one of ordinary skill in the art at the time the invention was made for the commands

of Peyret to include a MAC because it is a known procedure as disclosed in Hanel (Page 1).

11.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent

No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr,

U.S. Patent No. 5,974,529 as applied to claim 1 above, and further in view of Klingman, U.S.

Patent No. 5,729,594. Referring to claim 5, Peyret discloses a method for loading applications

onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig.

4). The smart card has a first interface system that may connect the smart card to the terminal

and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When

the smart card is connected to the terminal, the processor of the smart card, verifies the

authenticity of the terminal and of the server and visa versa. If the server and the smart card

authenticate each other, then the loader within the smart card begins the loading process (Col. 7,

lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of

commands to download the application component to the chipcard, to be loaded the smart card

authenticates the application code through the use of digital signatures (Col. 9, lines 50-53).

Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret

key or session key by the server, generation of a digital signature with the secret key or session

key by way of each command within the command sequence, transmission of the signed

command sequence as a data packet to the client. If the digital signature is valid then the

application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of

checking of the digital signature and execution of the commands if the digital signature is

correct. Chen discloses a method for installing an application wherein a desktop manager on the

user terminal unpacks the application program before installing the program on the memory card

(Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by

the client and transmission of the individual commands in sequence to the smart card. Zumkehr

discloses a system for error detection wherein individual program instructions are digitally

signed and later authenticated (Col. 2, lines 29-47). Peyret does not disclose communication

using SSL. Klingman discloses client server communications using SSL (Col. 3, lines 32-36). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

use SSL in the communications of Peyret in order to provide a secure communication line as

taught in Klingman (Col. 3, lines 37-39).

12.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent

No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr,

U.S. Patent No. 5,974,529 as applied to claims 1, 8 above, and further in view of Schneier.

Referring to claim 9, Peyret discloses a method for loading applications onto a smart card

wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card

has a first interface system that may connect the smart card to the terminal and second interface

to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is

connected to the terminal, the processor of the smart card, verifies the authenticity of the

terminal and of the server and visa versa. If the server and the smart card authenticate each other,

then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an

application is selected, which meets the limitation of loading a sequence of commands to

download the application component to the chipcard, to be loaded the smart card authenticates

the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures

utilize private or secret keys, which meet the limitation of delivery of a secret key or session key

by the server, generation of a digital signature with the secret key or session key by way of each

command within the command sequence, transmission of the signed command sequence as a

data packet to the client. If the digital signature is valid then the application is loaded onto the

smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature

and execution of the commands if the digital signature is correct. Chen discloses a method for

installing an application wherein a desktop manager on the user terminal unpacks the application

program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22),

which meets the limitation of unpacking of the data packet by the client and transmission of the

individual commands in sequence to the smart card. Zumkehr discloses a system for error

detection wherein individual program instructions are digitally signed and later authenticated

(Col. 2, lines 29-47). Peyret discloses the use of pubic key cryptography but does not disclose the

use of RSA. Schneier discloses that RSA is a form of public key cryptography (Page 366). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

use RSA as the public key cryptographic method in Peyret because RSA is the most popular

form of public key cryptography as disclosed in Schneier (Page 366-367).

Conclusion

13.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.
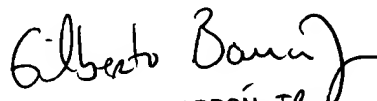
The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100